U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development, or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Internet Quarters Management Information System (iQMIS)
Bureau/Office: Office of the Secretary
Date: June 13, 2018
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Internet Quarters Management Information System (iQMIS) is a centralized web-based system used to set rental rates for employees or tenants living in government-owned housing, in accordance with Federal regulations in OMB Circular A-45, *Rental and Construction of Government Quarters*. The iQMIS application produces rent calculations and tenant rental

agreement documents as requested by the customers. iQMIS is offered as a shared service to assist Department of the Interior (DOI) bureaus/offices and Federal agency customers meet regulatory requirements. The purpose of iQMIS is to:

1. Set a rental rate for each Federal housing unit and tenant in compliance with A-45;
2. Track occupancy of each unit;
3. Print lease agreements and other documents for employees/tenants;
4. Provide rent payment forms/documents in order for the agency to collect rents;
5. Transmit payroll actions to the DOI Federal Personnel and Payroll System (FPPS) for employees;
6. Transmit estimates of rent revenues to the DOI Financial and Business Management System (FBMS) for each DOI rental unit; and
7. Produce housing occupancy, rent estimates and other reports for agency property managers.

There are numerous DOI bureaus/offices and Federal agency customers using iQMIS for employee housing. The DOI bureaus and offices using iQMIS include Bureau of Indian Affairs, Bureau of Land Management, Bureau of Reclamation, National Park Service, U.S. Fish and Wildlife Service, and U.S. Geological Survey.

C. What is the legal authority?

The legal requirement to charge employees and other occupants rent for Federal housing is provided in 5 U.S.C. 5911, Quarters and Facilities: Employees in the United States. The requirement specifying the amount of rent to be charged are identified in OMB Circular A-45, *Rental and Construction of Government Quarters,* and OMB Circular A-25, *User Fees*.

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name:*

010-00-02-02-2430-04, iQMIS System Security Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

iQMIS is not a system of records because records cannot be retrieved by an individual's name or other unique identifier. Users retrieve records by housing installation name and housing unit number. Rent collected from the employee/tenant through payroll deduction actions are processed through the DOI Federal Personnel and Payroll System (FPPS), which is maintained under the DOI-85: Payroll, Attendance, Retirement and Leave Records system of records notice, 73 FR 19090, April 8, 2008.

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

iQMIS records are primarily housing units and their occupants, and this data does not require an OMB Control Number. However, the IBC Quarters Program Office collects private rental market data, under a contract, to provide rents that comply with OMB Circular A-45, *Rental and Construction of Government Quarters*. Data from this market rental rate collection is stored in iQMIS. The collection of private rental market data from members of the public is covered by the Paperwork Reduction Act. OMB Control 1084-0033, Private Rental Survey, approves the collection of private rental market data from members of the public using OS-2000, "Private Rental Survey – Trailer Spaces" and OS-2001, "Private Rental Survey – Houses, Apartments, Mobile Homes." The OMB Control Number is approved every three years; currently valid to October 31, 2019.

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Truncated SSN

☒ Social Security Number (SSN)
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Employment Information
☒ Mailing/Home Address
☐ Other: *Specify the PII collected.*

For employees/tenants living in Federal housing, iQMIS users may request PII from the employee/tenant directly, the employee's hiring manager, or an Administrative Officer to ensure the payment of rent. For example, an individual's SSN or last 4 of the SSN are required to process a payroll deduction for rent. Mailing address is required to process a Bill of Collection for rent.

For iQMIS users, the iQMIS User Access Form collects name, bureau or agency, work email address, work location, work phone number, official job title, and office/branch/section. Username and password are collected by DOI's Active Directory to authenticate DOI employees that access the system through a web interface.

For members of the general public who complete the OS-2000 and OS-2001 forms, iQMIS collects address and telephone numbers of private rental unit agent/manager or owner/tenant (general public), which is mostly optional.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☒ Face-to-Face Contact
☒ Web site
☐ Fax
☒ Telephone Interview
☒ Information Shared Between Systems *Describe*

Electronic files are sent to the DOI Federal Personnel Payroll System (FPPS), and data is returned to iQMIS to confirm SSNs entered by iQMIS users and to match the correct name. This file sharing checks for inaccurate SSNs and avoids charging rent to the wrong employee. Files are also sent to FPPS after each pay period to specify ADD/CHANGE/STOP rent actions, and data is returned to iQMIS indicating what rent was paid and any errors.

For DOI bureaus and offices, electronic files are sent to the DOI Financial and Business Management System (FBMS). Electronic records are sent to FBMS in real time that contain the tenant name, housing unit, and rent data. This data is used to *estimate* rent revenues for Property/Buildings in FBMS. Data shared with FBMS is not used for billing or collection of rent. iQMIS also receives a nightly file from FBMS with Property/Building data. This data is used to keep FBMS and iQMIS Building data in sync. The file does not contain PII.

☐ Other: *Describe*

D. What is the intended use of the PII collected?

Specific business and payroll processes are determined by each agency, according to their unique requirements. SSNs are used to collect rent from the employee/tenant through payroll deduction actions, and are only collected for that purpose. Mailing address may be necessary to create a Bill for Collection. Emails and addresses may also be used to provide written and electronic communications with the employee/tenant on their rent, their lease, and other housing-related issues, for example, to provide a notice of inspection or to provide a notice of rent change.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

PII may be shared by the IBC Quarters Program Office to other IBC offices for payroll or accounting purposes. The IBC Payroll Operations Branch and IBC Debt Management Branch may require individual tenant names and SSN in order to assist with payroll deduction and rent issues. SSNs are only transmitted verbally or by Secure Transport, but never by email. All parties involved have a specific role in the rent payment process, and are a designated shared service provider. PII is also shared electronically between iQMIS and FPPS for rent payment purposes, as described in Section 2, question C above.

Each bureau owns their own iQMIS data and has a unique business process which prescribes how it will be used within their organization. They may share that data internally with their bureau Human Resources personnel, or with accounting personnel responsible for entering Bills of Collection into the accounting system. All personnel using employee/tenant PII have a "need to know" and a responsibility to secure the rent payment within their bureau/office process. These communications are conducted within their bureau/office, by email, face-to-face or via telephone.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

PII from one bureau/office is not typically shared with another bureau/office. However, a bureau may need to share PII with their shared service provider (IBC Payroll Operations Branch and the IBC Debt Management Branch), such as names and SSN in order to assist with payroll deduction and rent issues. SSNs are only transmitted verbally or by Secure Transport, but never by email. All parties involved have a specific role in the rent payment process. PII is also shared electronically between iQMIS and FPPS for rent payment purposes, as described in Section 2, question C above.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

PII from one agency is not typically shared with another agency.

PII may be shared verbally between an agency and the IBC Quarters Program Office, or verbally between the IBC Quarters Program Office and the IBC Payroll Office, to assist with agency payroll deduction issues. SSNs are only transmitted verbally or by Secure Transport, but never by email. All parties involved have a specific role in the rent payment business process.

PII may be shared between iQMIS and FPPS to facilitate rent deductions from payroll for Federal agency customers as part of the shared Federal services for these agencies. Each agency owns their own iQMIS data and has a unique business process which prescribes how it will be used within their organization. They may share that data internally with their agency Human Resources personnel, or with accounting personnel responsible for entering Bills of Collection into the accounting system. All personnel using employee/tenant PII have a "need to know" and a responsibility to secure the rent payment within their agency's process. These communications are conducted within their agency, by email, face-to-face or via telephone.

Sharing of PII is determined by each Federal agency customer business process for occupying housing. iQMIS users have access only to the data on their own housing installations and tenants that they are authorized in writing to manage. In other words, they can only share their own agency's data. All personnel using employee/tenant PII have a "need to know" and a responsibility to secure the rent payment within their Federal agency customer process.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Some agencies allow tribal organizations to use iQMIS for rent setting. Tribal iQMIS users only have access to their housing installations and tribal employees/tenants that they are authorized in writing to manage. Tribal iQMIS users may request PII from the employee, their hiring manager, or Administrative Officer in order to ensure that rent payment information is complete. These communications are typically by email, face-to-face or via telephone. This PII may be shared within their organization, for example, with tribal payroll personnel responsible for entering rent deductions into the payroll system, or with accounting personnel responsible for entering Bills of Collection into the accounting system.

☒ Contractor: *Describe the contractor and how the data will be used.*

Some agencies employ contractors to manage their iQMIS data. Each bureau/office or agency owns their own iQMIS data and has a unique business process which prescribes how it will be used within their organization. Contractor iQMIS users may request PII from the employee, their hiring manager, or Administrative Officer to ensure that rent payment information is complete. These communications are typically face-to-face or via telephone. This PII may be shared with the contracting agency payroll personnel responsible for entering rent deductions into the payroll system, or with accounting personnel responsible for entering Bills of Collection into the accounting system.

In addition, the IBC Quarters Program also contracts to collect private rental market data from property managers, landlords and tenants, using Form OS-2000 and OS-2001, approved under OMB Control Number 1084-0033, Private Rental Survey. The property address, information provider's name and phone number are collected and entered into iQMIS. Property managers, landlords, and tenants can decline to provide address, phone number, or other PII. They can, in fact, provide their first name only. This information is shared only with the Quarters Program Office and may be used to verify that the contractor is performing the work specified under the contract, and to determine the average time to complete the data collection form, as required by the OMB Paperwork Reduction Act.

☐ Other Third Party Sources: *Describe the third party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Occupancy of Federal housing is usually voluntary, but requires a contractual agreement or a lease, and the individual's agreement to pay rent for the housing provided. PII may be required to secure payment of rent. The necessary data is determined by the method of payment and each bureau/office or agency business process for collection of rent. At a minimum, the individual must provide their name.

Individuals entered into iQMIS have chosen to live in government housing at their work site. Employees are not required to live in government housing, and are free to seek housing elsewhere. Some employees are required to occupy housing as a condition of employment, but they voluntarily accept this condition when applying for the Federal position.

For bureaus/agencies that also use the FPPS, employee name and SSN are required for collection of rent by payroll deduction. In other agencies, the name and last four of the SSN may be required. If an employee declines to provide their SSN to their housing manager, the employee may be denied housing because payment cannot be arranged without the SSN. If an employee

refuses to provide their PII, other sources, such as the hiring manager or bureau/agency Administrative Officer, may be contacted for employee information.

For non-employees, at a minimum, their name and mailing address are required to establish the Bill of Collection. If these employees decline to provide their address, they will be denied housing since payment cannot be arranged in the accounting system without a billing address. Individuals may decline to provide personal phone numbers, email addresses, or mailing addresses. This information is typically optional.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement: *Describe each applicable format.*

☒ Privacy Notice: *Describe each applicable format.*

Privacy notice is provided through the publication of this privacy impact assessment. For members of the general public who respond to private rental market surveys, a privacy notice is provided in the OS-2000 and OS-2001 forms. Notice on the FPPS and DOI employee payroll processes, deductions and sharing is provided through the publication of the FPPS PIA and the DOI-85, Payroll, Attendance, Retirement, and Leave Records, system of records notice, 73 FR 19090, April 8, 2008.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

The Main web page in iQMIS provides searching tools. Because the primary system records are housing locations and housing units, users search for housing unit numbers they are authorized to manage. iQMIS users cannot search for or retrieve an individual name, SSN or other personal identifier from the system interface.

Individual tenant information is stored as a related record within each housing unit record and is not searchable. To find a specific tenant, the iQMIS user must know the tenant's current and previous housing unit number. However, iQMIS reports can be used to print employee/tenant name. SSNs do not print on Reports.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

The iQMIS system provides reports to help bureaus/offices and agencies with housing management and rent payment functions. All Users have access to reports, which they may also provide to their Supervisors and Managers.

Housing Unit reports provide information on whether a unit is occupied or vacant. These reports list the current tenant by name but do not include any other personal identifiers. Some examples of reports where the tenant name appears include:

- Current Tenants
- Rent by Tenant
- Rent Change by Tenant
- Rent Payment Method
- Tenant Occupation & Rent Payment Method

The iQMIS system also produces lease agreements and payroll deduction/payment forms for individual employees/tenants that may include PII. The processes are unique to each bureau/office and agency. The employee/tenant name will print on lease documents, but address or SSN is only printed on relevant documents to collect their rent payment through payroll (non-DOI agencies only, if entered by user), Bill for Collection, or internal account transfer. These documents may be provided to payroll or accounting personnel to ensure rent collection.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

iQMIS has internal validation that checks for completeness of data, but iQMIS cannot and does not verify accuracy. Each agency designates the appropriate iQMIS user who is responsible for accuracy, typically an on-site employee responsible for housing management. Each agency is the owner of their data, and is responsible for monitoring and ensuring the accuracy of their own data.

For the DOI bureaus and other agencies that use FPPS, iQMIS is able to confirm SSNs entered by users and confirm the correct name, see Section 2, question C above. This verification allows the system to detect inaccurate SSNs and ensures that rent is not charged to the wrong employee.

B. How will data be checked for completeness?

iQMIS has internal validation that checks for completeness of data (for example, SSN field must be 9 digits). iQMIS has built-in validation that also checks required fields for completeness. iQMIS records cannot be saved unless mandatory fields are complete. Users are warned if this occurs, and provided an opportunity to correct the issue and save the record again. Each user is ultimately responsible for its completeness, and each agency is responsible for monitoring and ensuring the completeness of their data.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Each agency is responsible for confirming the accuracy of tenant information and housing data. iQMIS users are responsible to ensure the data is current. For example, users will indicate when a tenant moves in or moves out, or whether a house has a government-furnished washer and dryer. Each agency is responsible for monitoring and policing that their data is current.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Bureaus and agencies using iQMIS are responsible for retaining their own signed lease agreements and property inventory changes, in accordance with applicable agency records retention schedules or General Records Schedules (GRS) approved by the National Archives and Records Administration (NARA). iQMIS users are responsible for properly filing and retaining housing-related documents, for 3 years after employee/tenant departure in accordance with GRS 5.4, Item 080, Housing rental and lease records. These records are temporary and destroyed three years after lease termination, lapse, reassignment, rejection of application, cancellation of lease, or conclusion of litigation.

Records regarding rent formulation and program management are maintained by the IBC Quarters Program Office under the Departmental Records Schedule (DRS) - 1, Administrative Records, Long-Term Financial and Acquisition Records, which has been approved by NARA (DAA-0048-2013-0001-0011). These records are temporary. The program is required to keep its rent-setting methodology and private rental market survey documentation for 6 years after cutoff. These records include private rental market data collected from the general public (managers/agents/landlords/tenants) through the OS-2000 and OS-2001 forms, and stored in iQMIS.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

An iQMIS System Administrator runs a procedure to remove PII from the database for any occupants that departed 6 years ago on an annual basis. PII must be retained for current occupants. Occupant name is retained for historical housing utilization purposes.

Approved disposition methods include shredding, acid leaching or pulping paper records, and degaussing or erasing electronic records in accordance with 384 Department Manual 1 and NARA guidelines.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a risk to privacy due to the volume and sensitivity of PII in the system. iQMIS is a FISMA moderate system based upon the type and sensitivity of data, and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. Privacy risks are mitigated by controls implemented in the system. iQMIS is an accredited Federal application that is protected by various physical, technical and administrative security controls, including continuous monitoring for security threats.

There is a risk that PII could be accessed or used by unauthorized personnel. This risk is mitigated through privacy and security controls and by limiting access to PII. Access controls are implemented to ensure that users are authorized to access the iQMIS system using the principle of least privilege and separation of duties. Authorized iQMIS users are responsible for bureau/office and agency property management controls, which require the collection of PII of occupants of government housing. Users are authorized by management in writing as having a responsibility in the rent payment and payroll deduction process, and to communicate with occupants on housing-related issues. Access to records in the system is limited to authorized personnel who have a need to know in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that individual's job responsibilities. Processes are unique to each agency. A payroll electronic record, or a printed Payroll Deduction Form, is used to initiate the rent payment, change the rent payment, or stop the rent payment after departure. If entered by the user, SSNs are encrypted in the database. An audit trail provides the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security. Only authorized users with valid DOI Active Directory credentials will be able to access the system. All iQMIS users are required to complete initial and annual privacy, security, and records management training, and sign DOI Rules of Behavior. It is the responsibility of their bureau/office and agency employer to provide privacy training.

There is a risk that information may be used outside the scope of the purpose for which it was collected. This risk is mitigated by limiting access to the system to only those personnel who have an official need to perform their job duties and ensuring employees complete initial and annual privacy, security, and records management training, and sign DOI Rules of Behavior. Agency payroll and accounting personnel have a business requirement to view and access PII to perform their official duties. PII is only disclosed to the authorized iQMIS user who is responsible for assigning housing, printing the employee/tenant lease, and collecting rent. Employee SSN and other PII may be collected and entered into iQMIS by authorized housing

personnel. iQMIS masks the SSN displayed on the screen using asterisks to ensure only authorized users can view the SSN. Individual users are responsible for protecting any privacy data in the paper form. SSN and other PII may be disclosed to payroll/accounting personnel for rent payment actions on a need-to-know basis. Payroll actions are automated through a file interface to FPPS. Transmission of files between iQMIS and FPPS is tightly controlled, and both systems are accredited Federal applications. PII is used only for internal payroll and accounting purposes which is not shared outside the Department unless authorized.

There is a risk that individuals may not have adequate privacy notice. This risk is mitigated by the publication of this PIA, and the related DOI-85: Payroll, Attendance, Retirement and Leave Records system of records notice for payroll processes. A privacy notice is also provided on the OS-2000 and OS-2001 forms.

There is a risk that information may be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. The data collected and stored has intentionally been limited to the minimal amount of data needed to assigning housing, manage employee/tenant lease, collect rent, and manage government housing program reporting and meet Federal requirements. Records are maintained in accordance with records schedules that were approved by NARA. Users also are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Description*

The data in iQMIS is required for the computation of employee rental rates in accordance with OMB Circular A-45, *Rental and Construction of Government Quarters*, and helps to support each agency's housing management and rent payment processes. Any PII in iQMIS is relevant and necessary in order to collect rent from the tenant in accordance with the bureau/office or agency payroll/accounting business process or to provide the tenant with housing- and rent-related correspondence.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

The system does not derive new data or create previously unavailable data about an individual.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☐ System Administrator
☒ Other: *Describe* System Managers, Database Administrators

Users receive access approval in writing from their bureau/agency Supervisor and a second-level manager. Users must agree in writing to the iQMIS Rules of Behavior. They complete an initial and annual privacy, security, and records management training, provided by their own bureau/agency. A User's ability to change data is specified on the authorization, based on their responsibilities for housing management and designated system Role, see Section 4, question H. Record access is limited in iQMIS to the specific housing installation(s) they manage. Remote access is not authorized.

Contractors receive access approval in writing from a bureau/agency Supervisor and a second-level manager. Contractors must agree in writing to the iQMIS Rules of Behavior. They

complete an initial and annual privacy, security, and records management training, provided by the contracting bureau/agency. A contractor's ability to change data is specified on the authorization, based on their responsibilities for housing management and designated system Role, see Section 4, question H. Record access is limited in iQMIS to the specific housing installation(s) they manage.

Developers are in house IBC Quarters Program employees with responsibilities to operate and maintain the iQMIS system and program its functionality and security features. Developers receive access approval in writing from their IBC Supervisor and a second-level manager. Users must agree in writing to the iQMIS Rules of Behavior. They complete an initial and annual privacy, security, and records management training. A Developer has the ability to view or change any data in the system, in addition to having complete authority over program functions. Developers do not normally change data, but may do so in order to resolve an issue.

System Managers are internal IBC Quarters Program employees with responsibilities to operate and maintain the iQMIS system, enter rent algorithms, and provide Help Desk services to users. System Managers receive access approval in writing from their Supervisor and a second-level Manager. Users must agree in writing to the iQMIS Rules of Behavior. They complete an initial and annual privacy, security, and records management training. In order to assist with issues and problems, they have access to all data in the system. System Managers do not normally change data, but may do so in order to resolve an issue.

Database Administrators are DOI OCIO employees with responsibilities to operate and maintain the Oracle database tables. SSNs are encrypted in the Oracle tables, but other non-sensitive PII, such as phone number, email or mailing address, are not. Database Administrators do not change data, although they have the capability to do so.

The DOI/OCIO backs up all IBC server files, including iQMIS, using an external tape drive system. Tapes are transported to an off site storage facility for disaster recovery purposes. This process is tightly controlled. SSNs are encrypted in the Oracle tables, but other non-sensitive PII, such as phone number or mailing address, are not.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access is based on the user roles defined in the system and the completed, approved iQMIS User Access Request form. Below is a list of user access roles:

- System Manager – Members of the IBC Quarters Program Office that maintain the application and operate the iQMIS Help Desk.
- Policy Manager – Department of Interior system owner, Quarters Policy Manager, and Chairman of the National Housing Council with the ability to view (read-only) housing data for all agencies. A Policy Manager cannot view or print SSNs.
- Security Manager – Members of the IBC Quality Assurance Section that manage all user access based on a completed iQMIS User Access form with agency authorization. A

Security Manager cannot view any housing or tenant data, and therefore has no access to PII.

- Comparable Manager – User collects industry housing data and uploads data to iQMIS; typically a contractor. A Comparable Manager is only uploading private rental market data they have collected. This user cannot view any government housing or tenant data, and therefore has no access to PII.
- Housing Manager – Users manage housing and tenant data for their agency. If they are responsible for collecting PII, they will enter the data and process rent payments.
- Tenant Manager – Users manage tenant data for their agency. They are responsible for collecting PII, and will enter the data and process rent payments.
- Read Only – Users with the need to view housing data for their agency (read only role). A Read Only Manager cannot view or print SSNs.

Each user also has a scope of authority to define the housing installation(s) they can view or revise.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act contract clauses are in the contract with the contractor that supports the IBC Quarters Program. This contractor collects private rental market data on the OS-2000 and OS-2001 forms, and uploads the form data into iQMIS. These contractors are also considered users of the system. Some agencies hire contractors to support use of iQMIS to enter housing inventory data and tenants/employees living in housing. Additionally, OCIO may hire contractors to provide maintenance of the system under a hosting agreement with iQMIS, such as virus scans, patching, and intruder protection.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

iQMIS identifies its authorized users and tracks their last login date. Individual iQMIS user information contains only name, work city, work email, and work phone, which are entered into their profile. iQMIS records all changes made by each user to their housing, tenant, and rent data

using an audit trail. These changes are displayed within iQMIS web pages and available in reports. iQMIS records the date changed, the user who changed the data, the field(s) changed, the previous value of each field changed, and the new value of each field changed. Audit reports available include:

- Housing Audit Report – All changes to housing or tenant data, reportable by a selected date range
- User Audit Report – User password resets, changes to user profile by Security Manager, reportable by a selected date range iQMIS is capable of reporting invalid and valid logins, current users, and inactive users.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The system conducts normal auditing of system users and user activities within the system. Each housing/tenant record audit trail displayed on a web page reflect changes to a field, including date changed, the user who made the change, the field changed, the old value, and the new value. Each user record audit trail (for system and security managers only) will document a user password reset, plus user scope, role or contact changes made by a Security Manager.

M. What controls will be used to prevent unauthorized monitoring?

Controls outlined in the iQMIS System Security Plan that adhere to the standards outlined in the National Institute of Standards and Technology (NIST) SP 800-53, *Recommended Security and Privacy Controls for Federal Information Systems*, are in place to prevent unauthorized monitoring. These controls include the use of role-based training, encryption, and maintaining data in secured facilities. iQMIS assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

Routine scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any iQMIS assets. iQMIS IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Cards

☒ Locked File Cabinets
☒ Secured Facility
☐ Closed Circuit Television
☒ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Director, Office of Acquisition and Property Management, is the iQMIS Information System Owner and the official responsible for oversight and management of the iQMIS security controls and the protection of agency information processed and stored in the iQMIS system. The Information System Owner and Information System Security Officer are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in the iQMIS system. These officials

and authorized iQMIS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act for DOI, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendment, as well as processing complaints, in consultation with DOI Privacy Officials.

Customer agency data in the system is under the control of the customer, and the customer is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

Each user is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of their employees/tenants privacy protected data to their own bureau/agency in accordance with their procedures. Per the iQMIS Rules of Behavior, iQMIS Users must "Notify the iQMIS Help Desk and appropriate bureau/agency IT personnel immediately of any security events or incidents that might threaten or negatively impact the integrity or availability of iQMIS. The bureau/agency will ensure that policy and procedures are in place such that apparent security violations are to be investigated and remedial action taken."

The iQMIS Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, and ensuring to the greatest possible extent that agency data is properly managed and that all access to data has been granted in a secure and auditable manner. The iQMIS Information System Owner, Information System Security Officer, and authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, the customer agency and appropriate DOI officials in accordance with Federal policy and established DOI procedures. Each customer agency is responsible for the management of their data and reporting of any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data.